**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *draft\_S3-232088-r3***

**Electronic meeting, Online, 17 - 21 April 2023**

**Source: Nokia, Nokia Shanghai Bell, Qualcomm Incorporated ?, LG Electronics?**

**Title: evaluation for KI#3 network slice admission control**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***Approve the evaluation to TR33.886***

# 2 References

[1] 3GPP TR 23.700-41 “Study on enhancement of network slicing; Phase 3”

[2] 3GPP TR 33.886 "Study on enhanced security for Network Slicing Phase 3"

# 3 Rationale

The contribution proposes evaluation for solution#2 to mitigate security risks caused by potential threats triggered by malicious/compromised NSACFs in specific serving areas.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st change \*\*\*\*\*\*\*\*\*\*\*\*

### 5.2.3 Evaluation

Editor’s Note: Further alignment with SA2 work is may be needed.

The solution addresses KI#3 network slice admission control (NSAC) to mitigate the risk that malicious/compromised NSACF(s) in specific area(s) of a PLMN or in a VPLMN may launch DoS attack towards the Primary NSACF. The solution proposed that the primary NSACF validates the number of UEs/PDU sessions for a S-NSSAI when received NSAC\_NumberOfUE/PDUsUpdate\_Request from a NSACF. The primary NSACF validates the number by comparing the number from the (distributed) NSACF and numbers from UDM.

This solution does not prevent the AMF/SMF providing incorrect information to both the UDM and vNSCAF to provide incorrect information on slice usage. However with home control proposed in the solution, the issue caused by the AMF/SMF providing incorrect information to the vNSCAF can be partially mitigated,

For example, a malicious SMF may provide incorrect information on slice usage to UDM, that may impact the accuracy of PDU session numbers of a slice reported by UDM in some extent. However, with security feature introduced in 5G for linking home control to subsequent procedures during/after primary authentication procedures (see 6.1.4 of TS 33.501), and authorization on slice usage for a UE, as well as feature for limiting number of PDU sessions for a registered UE, the contribution of malicious AMF/SMF to the DoS attack in NSAC case can be limited, and its influence on the decision of primary NSACF can be restricted but not fully prevented.

Impacts on existing entities and interfaces:

Primary NSACF:

* be capable to get number of registered UEs/PDU sessions for a network slice in specific VPLMN or AMF/SMF from UDM and validate the number from (distributed) NSACF with numbers from UDM.

NOTE: how does the Primary NSACF validate the numbers from (distributed) NSACF with numbers from UDM, and handle the abnormal scenario are implementation dependant.

UDM:

* support an new service to report number of registered UEs/PDU sessions for a network slice in specific VPLMN or AMF/SMF.

Editor’s Note: How does UDM acquire the number of registered UEs for a S-NSSAI is FFS

gNB: None

UE: None

\*\*\*\*\*\*\*\*\*\*\*\*\* End of the changes \*\*\*\*\*\*\*\*\*